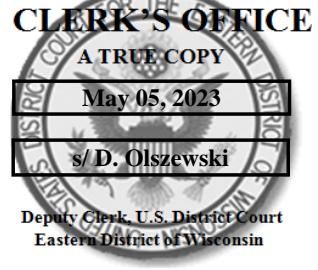


UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF WISCONSIN



In the Matter of the Seizure of
(Address or brief description of property or premises to be seized)

APPROXIMATELY 456,995.14843 USDT, AND ANY OTHER
FIAT CURRENCY AND ALL FORMS OF CRYPTOCURRENCY,
ON DEPOSIT IN BINANCE ACCOUNT USER ID #197016535,
HELD IN THE NAME OF NICOLAS ROZO-JIMENEZ

Case Number: 23 MJ 75

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, Kellen J. Williams, being duly sworn depose and say:

I am a Special Agent with the Drug Enforcement Administration, and have reason to believe that in the Northern District of California there is now certain property, namely, approximately 456,995.14843 USDT, and any other fiat currency and all forms of cryptocurrency, on deposit in Binance account user ID #197016535, held in the name of Nicolas Rozo-Jimenez, that is (1) civilly forfeitable under 21 U.S.C. § 881(a)(6), and criminally forfeitable under 21 U.S.C. § 853, as proceeds of distribution of controlled substances committed in violation of 21 U.S.C. § 841; and (2) civilly forfeitable under 18 U.S.C. §§ 981(a)(1)(A), and criminally forfeitable under 18 U.S.C. § 982(a)(1), as funds involved in money laundering transactions and unlicensed money transmitting in violation of 18 U.S.C. §§ 1956, 1957, and 1960, and which property is therefore also subject to seizure for purposes of civil forfeiture under 18 U.S.C. § 981(b), and for purposes of criminal forfeiture under 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(f).

The application is based on these facts:

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

KELLEN WILLIAMS
Digitally signed by KELLEN WILLIAMS
Date: 2023.05.04 18:48:36 -05'00'

Signature of Affiant
Kellen J. Williams, DEA

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone and email.

5/5/2023 at 1:49 PM
Date and time issued

at Milwaukee, Wisconsin
City and State

William E. Duffin, U.S. Magistrate Judge
Name & Title of Judicial Officer


Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A SEIZURE WARRANT

I, Kellen J. Williams, being duly sworn, do hereby depose and state:

I. BACKGROUND, TRAINING, AND EXPERIENCE

1. I am a Special Agent with the Drug Enforcement Administration (DEA), and I am currently employed as a DEA Special Agent, and have been since September 2012. I am currently assigned to the Milwaukee District Office, Enforcement Group 61, which is located in the Eastern District of Wisconsin. Over the course of my career, I have received specialized training about drug trafficking and money laundering from the U.S. Department of Justice. My career has included long terms of special investigative assignments in drug enforcement and money laundering. I have conducted numerous drug conspiracy and money laundering investigations in the United States and abroad.

2. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have participated in numerous investigations related to illegal drug trafficking, among other things, have conducted or participated in surveillances, the execution of search warrants, and debriefings of informants related to drug trafficking and money laundering. I have drafted affidavits for search warrants including tracking of vehicles, cellular phones, and searches of residences and electronic devices. I also consult with other agents with extensive experience in drug trafficking investigations. As a result, I am familiar with common practices to promote and facilitate drug trafficking.

3. Based on my training and experience, I am aware of the following:

A. Drug trafficking organizations (DTOs) generate large amounts of cash proceeds in the U.S. and elsewhere. In order to repatriate their cash proceeds from the U.S. and other countries back to their country of origin where they can be used by the DTO members, DTOs often employ professional money launderers. For a fee, professional money

launderers provide the DTO with currency in the DTO's native country in exchange for bulk currency in the country where the DTO's narcotics are distributed.

B. Professional money launderers utilize a variety of methods to accomplish their goals including trade-based money laundering, bulk currency smuggling and virtual currency trading to achieve their goals.

C. Virtual currency, also known as cryptocurrency, is generally defined as an electronically sourced unit of value that can be purchased with, sold for, or used as a substitute for fiat currency (i.e., currency created and regulated by a government). Cryptocurrency is not issued by any government, bank, or (with limited exceptions) companies. It is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Cryptocurrency can be quickly transmitted directly between parties and across national borders, without the need for a facilitating third party like a traditional financial institution. Many cryptocurrencies, including Bitcoin and Tether, operate via a "blockchain," a record (or ledger) of every transaction ever conducted that is distributed throughout the network. The blockchain will not list the names of parties to the transaction but will list the date and time of the transaction, the originating and receiving public address, and how much cryptocurrency was transferred.

D. For example, Bitcoin is a type of virtual currency, circulated over the Internet as a form of value. As stated on its website, "Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network." See <https://bitcoin.org/en/>. The website (at <https://bitcoin.org/en/how-it-works>) further explains the ease of getting started with Bitcoin:

As a new user, you can get started with Bitcoin without understanding the technical details. Once you have installed a Bitcoin wallet on your computer or mobile phone, it will generate your first Bitcoin address and you can create more whenever you need one. You can disclose your addresses to your friends so that they can pay you or vice versa. In fact, this is pretty similar to how email works, except that Bitcoin addresses should be used only once.

E. The technology underlying Bitcoin utilizes "public key cryptography," a mathematical algorithm that generates a pair of unique, corresponding keys: the "public key" and the "private key." These components form the "public address," which is used to send and receive Bitcoin and can be shared with whomever wants to send Bitcoin to that address. A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Bitcoin are sent to and received from Bitcoin "addresses." Individual cryptocurrency addresses are controlled through the utilization of a unique private key, which can be thought of as a

password used to access the address. The private key limits access to only the owner of the cryptocurrency address.

- F. A Bitcoin public address has been compared to the mailing address of a locked post office (P.O.) box. Whomever the P.O. box belongs to can share that mailing address freely. For example, a company can advertise their P.O. box's mailing address on invoices, so customers know where to send their envelopes full of cash. The company need not worry that customers could then open the P.O. box (and take the cash inside), because that would require the means to unlock the box, such as a physical key. A private key function like that physical key: whomever controls it controls all funds that have been deposited into the associated public address.
- G. A cryptocurrency wallet may contain multiple cryptocurrency addresses. Ownership of a cryptocurrency wallet denotes stewardship of the multiple addresses therein.
- H. Wallets can be backed up in a number of ways. The digital files associated with the wallet might be stored locally on the user's computer or stored remotely in the cloud. Alternatively, a user can generate a "recovery seed," a pseudo-random collection of approximately 12-24 natural language words from which wallet software can mathematically derive all of their public addresses and private keys, allowing the user's wallet to be recreated on any computer or smartphone. A recovery seed can be stored, for example, in a digital text file on a computer or smartphone or written on a piece of paper. If a user retains a copy of their recovery seed, they retain control of their cryptocurrency, regardless of any devices law enforcement decides to seize, unless and until the latter are able to move the funds to a new, government-controlled wallet.
- I. Cryptocurrency can also be stored on a hard wallet, a device like a USB thumb drive that keeps all the accounts off-line. This helps prevent hackers from getting to the cryptocurrency. Hard wallets work by storing the private key, keeping it off the Internet and therefore mitigating the risks of cryptocurrency being compromised in an online attack. A hard wallet can be used to conduct a transaction when it is plugged into a computer, unlocked with a PIN or passphrase, and then connected to the internet to initiate the sending or receipt of funds. If a hard wallet is lost or stolen, the private key can be regenerated using a recovery seed. This recovery seed enables the user to move the private keys to a new hard wallet.
- J. It is possible using the blockchain to trace funds forwards and backwards from a single address or a single transaction, not unlike the manner in which investigators trace the movement of funds in fiat currencies.

- K. Despite the anonymized nature of a cryptocurrency blockchain, information identifying the sender, or the recipient of a transaction can be obtained from payment processors or vendors. This information helps investigators identify payment streams – a single flow of funds over time – believed to belong to the same pool of funds controlled by individuals; and
- L. Bad actors sometimes utilize services to further obfuscate the movement of funds. A cryptocurrency tumbler or cryptocurrency mixing service is a service that mixes cryptocurrency funds with funds belonging to other individuals, so as to obscure the trail back to the fund's original source. When cryptocurrencies are tumbled or mixed, the mixer will take the cryptocurrency from several different users and run them through an algorithm that mixes those funds together, and then redistributes them to the users. For example, one hundred users send 0.1 bitcoin to a new address, aggregating those funds into one big transaction. The funds are subsequently distributed among the hundred users, each of them receiving 0.1 "clean" bitcoin. As a result, tumbled or mixed cryptocurrencies lose many of the attributes that make cryptocurrencies traceable.

II. PURPOSE OF AFFIDAVIT AND PROPERTY TO BE SEIZED

4. For the reasons set forth below, I submit this affidavit in support of an application for a seizure warrant to seize up to approximately 456,995.14843 USDT held in the Binance account belonging to Nicolas ROZO-JIMENEZ, Binance user ID 197016535 ("Target Account 2"), and up to approximately 60,000 USDT held in the Binance account belonging to Juan Esteban ARDILA-LONDONO, Binance User ID 27815331 ("Target Account 3").¹

5. For the reasons set forth below, I submit that up to 459,995.14843 USDT held in the **Target Account 2** and up to 60,000 USDT held in the **Target Account 3** are:

- a. Funds traceable to, and are therefore proceeds of, distribution of controlled substances, committed in violation of 21 U.S.C. § 841, and therefore are subject to civil forfeiture under 21 U.S.C. § 881(a)(6), and subject to criminal forfeiture under 21 U.S.C. § 853(a);
- b. Funds involved in, or traceable to funds involved in, unlicensed money transmitting, committed in violation of 18 U.S.C. § 1960, and therefore are

¹ Target Account 1 was closed by Binance in March of 2023, see paragraph 53.

subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A), and subject to criminal forfeiture under 18 U.S.C. § 982(a)(1);

- c. Funds involved in, or traceable to funds involved in, money laundering offenses, committed in violation of 18 U.S.C. §§ 1956 and 1957, and therefore are subject to civil forfeiture under 18 U.S.C. §§ 981 (a)(1)(A), and subject to criminal forfeiture under 18 U.S.C. § 982(a)(1); and
- d. Subject to seizure via a civil seizure warrant under 18 U.S.C. § 981(b) and via a criminal seizure warrant under 18 U.S.C. § 982(b)(1) and 21 U.S.C. § 853(f).

6. This warrant request is connected with an ongoing criminal and financial investigation in the Eastern District of Wisconsin regarding Luis Ernesto OCEGUERA-TIRADO, Angel VELAZQUEZ-BRAVO, Alfredo CUELLAR-FISHER, Jose TORRES-ESPANA, Francisco GRANADOS-ARAQUE, Giovanny COLORADO-RESTREPO, Nicolas ROZO-JIMENEZ, Juan Esteban ARDILA-LONDONO and others. For the reasons discussed below, case agents believe that OCEGUERA-TIRADO, VELAZQUEZ-BRAVO, CUELLAR-FISHER and TORRES-ESPANA are Mexican money launders specializing in cryptocurrency. GRANADOS-ARAQUE utilizes the money laundering networks of OCEGUERA-TIRADO and VELAZQUEZ-BRAVO to arrange for the bulk cash pick-ups in the United States. Based on their training and experience, and the investigation to date, case agents believe that Giovanny COLORADO-RESTREPO, owner of **Target Account 1**, Nicolas ROZO-JIMENEZ, owner of **Target Account 2**, and Juan Esteban ARDILA-LONDONO, owner of **Target Account 3**, are involved in money launderer specializing in cryptocurrency.

III. PROBABLE CAUSE

A. Drug Trafficking Investigation of Clayton, Mathis, and Teran-Vargas

7. Information contained in this affidavit has been compiled through my own investigative efforts as well as the investigative efforts and knowledge from other law enforcement officers and

intelligence analysts (“case agents”). This affidavit is not all-inclusive, and facts contained in this affidavit are believed to sufficiently establish probable cause to seize the **Target Accounts**.

8. The DEA has been investigating the OCEGUERA-TIRADO Drug Trafficking and Money Laundering Operation (DTMLO) since approximately November 2020. OCEGUERA-TIRADO is believed to be the head of the DTMLO and VELAZQUEZ-BRAVO, CUELLAR-FISHER, TORRES-ESPANA and GRANADOS-ARAQUE are believed to be close associates and money launderers.

9. On August 20, 2020, the Federal Bureau of Investigation (FBI) National Threat Operations Center received an online tip via tips.fbi.gov regarding potential international drug trafficking and tax evasion. The tip identified Dwight CLAYTON and stated that individuals are using a business called S&C Trucking LLC to hide proceeds in Milwaukee, Wisconsin. The tip stated a second unidentified person owes a large sum of money for income taxes and owes child support and started a business to get paid “under the table” from a source. The tip stated this second person ran income through that source and uses his girlfriend’s accounts to hide profits from drug trafficking. The tip further stated that this second person is involved in drug trafficking with the people who operate S&C Trucking LLC, 1918 East Lafayette Place #309, Milwaukee, Wisconsin, and is a co-owner of the business. The tipster identified this person as Dwight CLAYTON. The tip stated that the business is registered “with the DOT under a different address which is a home.” The tipster further reported that CLAYTON had been sent to prison for federal drug charges in the past. According to the tip, CLAYTON and the second person lived lavish lifestyles and clearly lived beyond their means.

10. A search of Wisconsin Department of Financial Institutions records revealed that Dwight CLAYTON is the registered agent of S&C Trucking LLC. The LLC address listed for the business is 9736 West Tower Avenue, Milwaukee, Wisconsin. Case agents conducted surveillance at this

location on several occasions and have never seen a person or vehicle come or go from the residence. Additionally, cameras are mounted on the exterior of the residence and all of the window blinds are closed. I am aware, based on my training and experience, that drug traffickers frequently maintain “stash” houses which are residences used to store drugs prior to distribution and/or to store proceeds of drug sales after distribution. These residences typically have little vehicle or pedestrian traffic so as to avoid drawing attention to the house. Additionally, cameras are often mounted to the exterior of “stash” houses to allow the drug trafficker to observe if the residence is being approached by police or rival drug traffickers.

11. On October 20, 2020, Texas Department of Public Safety investigators were conducting surveillance at a suspicious business in Pharr, Texas. Investigators observed an open overhead garage door at the business warehouse and observed a pallet containing several boxes sitting next to a pickup truck in the business. The rest of the warehouse appeared to be empty. A short time later, a truck belonging to Estes Express Lines arrived, loaded the pallet onto a truck, and left the business. Investigators maintained surveillance until the truck arrived at the Estes Express Lines property. Investigators subsequently approached the employees of the company and inquired about the pallet. Investigators were provided with the bill of lading related to the shipment. The bill of lading indicated that the pallet contained 492 pounds of optical cable and was being shipped from Dixie Cable, 2003 North Veterans Boulevard, Suite 18, Pharr, Texas 78577 to Raul Gallegos, 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin 53212. The shipper’s name was listed as Carlos Trevino with phone number (956) 996-2424. The recipient was listed as Raul Gallegos with phone number (657) 261-1934. Investigators conducted a K-9 sniff of the pallet and received a positive alert for the presence of controlled substances. A subsequent search of the pallet revealed approximately 60 kilograms of cocaine concealed within the boxes on the pallet.

12. Shipping records revealed that three prior shipments had been sent from Pharr, Texas to 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin 53212. Two of those shipments had been picked up at the shipping company and one had been delivered on August 14, 2020, to 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin 53212. Case agents obtained surveillance video from North Shore Bank which showed that on August 14, 2020, Dwight CLAYTON arrived at the side of the business at 1850 North Martin Luther King Jr. Drive, driving a black Dodge Ram 2500 pickup. The bed of the pickup was empty upon his arrival. A short time later, a box truck driven by the shipping contractor arrived and parked on the side of the business. CLAYTON was observed positioning the Dodge Ram near the shipping company vehicle. A short time later, CLAYTON drove away from the area. The bed of the Dodge Ram now contained what appeared to be a shipping pallet. This pallet was similar in appearance to the pallet seized in Pharr, Texas on October 20, 2020.

13. A search of Wisconsin Department of Financial Institutions records revealed that Peachy Clean Commercial and Construction Cleaning LLC lists its office address as 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin 53212. The registered agent is Ronny Thompson. Numerous law enforcement database searches identified Ronny Thompson's phone number as (414) 803-9676.

14. According to AT&T records for (414) 469-6235, the number used by Dwight CLAYTON, the phone is subscribed to Dwight CLAYTON at 9736 West Tower Avenue, Milwaukee, Wisconsin. An analysis of the records for (414) 469-6235 revealed that CLAYTON was in contact with (414) 803-9676, the number used by Ronny Thompson, 153 times from March 5, 2020, through October 8, 2020. An examination of records for (414) 469-6235 also revealed that CLAYTON was in regular and frequent contact with other phones known to be used by drug traffickers in the Milwaukee area.

15. A search of Public Access to Court Electronic Records (PACER) records revealed that on April 12, 2005, Dwight CLAYTON was convicted in Case # 04-CR-66 of Conspiracy to Possess with Intent to Distribute Five Kilograms of Cocaine and Money Laundering. CLAYTON was sentenced to 108 months of imprisonment on each count with the sentences to run concurrently.

16. On November 2, 2020, the Honorable William E. Duffin, United States Magistrate Judge in the Eastern District of Wisconsin, signed a tracking warrant for a silver 2015 Kia Optima, bearing Wisconsin license plate ACV-2064, known to be driven by Dwight CLAYTON. On November 24, 2020, case agents observed that the Kia left 9736 West Tower Avenue, Milwaukee, Wisconsin, and travelled directly to a vacant lot in the 4700 block of South Packard Avenue, Cudahy, Wisconsin. Case agents responded to that area to conduct surveillance of the Kia. At 3:27 p.m., case agents observed that the Kia had travelled to the parking lot of a BMO Harris Bank located at 4677 South Packard Avenue, Cudahy, Wisconsin. Case agents conducted surveillance of the Kia and observed CLAYTON in the driver's seat and a second unidentified male in the front passenger seat. The second male appeared to be looking down at the passenger-side floorboard. At 3:35 p.m., the Kia drove out of the BMO Harris parking lot and drove back to the 4700 block of South Packard Avenue. The Kia did a U-turn and pulled to the curb on the south side of the street. Case agents observed the unidentified male exit the front passenger seat and retrieve a small rolling suitcase and a small duffel bag from the vehicle. The male then entered the JP Morgan Chase Bank at 4702 South Packard Avenue, Cudahy, Wisconsin. CLAYTON drove the Kia out of the area and was not followed.

17. The unidentified male approached a teller window and appeared to be conducting a lengthy transaction. At 4:34 p.m., the male exited the bank and stood in front of the bank looking at his cellular phone. At 4:42 p.m., a vehicle displaying an Uber sticker arrived in front of the bank. The male opened the rear cargo area of the vehicle and placed the suitcase and the duffel bag into the

vehicle. Case agents followed the vehicle to the Hilton Garden Inn – Milwaukee Airport, 5890 South Howell Avenue, Milwaukee, Wisconsin, where the male exited the vehicle and entered the hotel.

18. Case agents interviewed employees at the JP Morgan Chase Bank who stated that the male had made a large cash deposit but provided no additional information about the transaction. A subpoena served on JP Morgan Chase later revealed that the male had deposited \$169,650 in United States currency to an account held by Redzien LLC, a business organized in the State of Florida. The authorized signers on the account are Kevin MATHIS and Hector Manuel TERAN-VARGAS. Banking records for this account show that the account was opened on September 23, 2020. A search of Florida corporation records identified the registered agent for Redzien LLC as Kevin MATHIS, of 10870 West Sample Road # 4504, Coral Springs, Florida. The Articles of Organization for Redzien LLC identify MATHIS and Hector M. VARGAS, a.k.a Hector TERAN-VARGAS, as Managers of the LLC. Additional banking records identified MATHIS' phone number as (941) 809-5186 and email address is kmathis193@gmail.com and TERAN-VARGAS' phone number as (832) 212-3490. An Administrative Subpoena served on T-Mobile identified the subscriber to (941) 809-5186 as Conceptual Design & Consulting Services Inc, of 193 Medici Ter, North Venice, Florida, and the customer's name as "Mathis" and the subscriber to (832) 212-3490 as "Hector Teran" of 8152 Emerald Forest Court, Sanford, Florida 32771. Telephone records reveal that MATHIS, using (941) 809-5186, is in regular and frequent contact with TERAN-VARGAS, using (832) 212-3490.

19. Banking records revealed that Redzien, LLC also opened bank accounts at Bank of America, Wells Fargo Bank, and Regions Bank. A review of transactions for these banks, and JP Morgan Chase Bank, identified approximately 106 suspicious transactions totaling \$21,268,257 from June 18, 2020, through March 24, 2021. These transactions occurred in at least twenty-one different states, including Wisconsin. On January 20, 2021, case agents spoke to a representative of Bank of

America's Global Financial Crimes Investigations – Anti-Money Laundering department. The representative advised that from November 23, 2020, thru January 5, 2021, Kevin MATHIS and Hector TERAN-VARGAS had deposited approximately \$1,000,000 into accounts at Bank of America. Bank of America subsequently closed those accounts due to suspicions that the accounts were being used for money laundering.

20. Records indicate that soon after these deposits are made, money is wired out of the account to brokerage accounts of companies in Mexico and the British Virgin Islands. Furthermore, case agents have identified a large amount of cryptocurrency deposits and subsequent transactions made by TERAN-VARGAS on the cryptocurrency exchange Binance.

21. On December 2, 2020, case agents went to the Hilton Garden Inn – Milwaukee Airport and reviewed hotel registration records for November 24, 2020. Those records revealed that Kevin MATHIS had rented room 339 for one night on November 24, 2020. MATHIS checked in to the room at 4:52 p.m., approximately the same time case agents observed the Uber drop the male off at the hotel. MATHIS checked out of the hotel at 3:42 a.m., the following morning. A review of telephone records for (941) 809-5186 revealed that a call was placed to the Hilton Garden Inn – Milwaukee Airport on November 24, 2020. Based on their training and experience, and the investigation to date, case agents believe this call involved MATHIS reserving a room for that evening.

22. Case agents believe, based on the numerous, large cash deposits followed by wire transfers to foreign accounts, travel throughout the United States in furtherance of money laundering, and the lack of a legitimate business purpose for large cash transactions involving Redzien, LLC (a mining business), that Kevin MATHIS and Hector TERAN-VARGAS are involved in laundering of drug proceeds throughout the United States, including in the Eastern District of Wisconsin.

B. Identification of Luis Ernesto Oceguera-Tirado and Angel Velazquez-Bravo

23. In December 2020, an Administrative Subpoena was served on T-Mobile, requesting historical call records for (832) 212-3490, used by TERAN-VARGAS. Case agents analyzed the records and found TERAN-VARGAS to be in frequent and regular contact with Mexican phone number +52 331 278 6140. Case agents conducted an open search of +52 331 278 6140 and found an open Facebook post by Luis Ernesto OCEGUERA-TIRADO written on July 12, 2019, describing a lost cat and posting his phone number of (+52) 331 278 6140. An open search of OCEGUERA-TIRADO revealed he is associated with Grupo Gueratti, an investment management company based in Guadalajara, Jalisco, Mexico. Further database searches reveal OCEGUERA-TIRADO is associated with Twitter account @netogueratti, an account which frequently discusses and promotes cryptocurrency, including a post made on May 29, 2020, stating “The largest Crypto Exchange Worldwide. BINANCE.” Based on their training and experience and the investigation to date, case agents believe OCEGUERA-TIRADO is involved in cryptocurrency transactions with TERAN-VARGAS.

24. Beginning in approximately July 2021, CS-1 began providing information to the Milwaukee District Office (MDO) about the Luis Ernesto OCEGUERA-TIRADO DTMLO. CS-1 told investigators that OCEGUERA-TIRADO is a leader of a DTMLO who resides in Mexico City and Guadalajara, Mexico, and has been laundering drug proceeds since at least June 2020. According to CS-1, in the past OCEGUERA-TIRADO has asserted his DTMLO launders proceeds for Colombian and Mexican-based drug trafficking and money laundering organizations that have cells operating in countries around the world, including the United States. CS-1 confirmed that Hector TERAN-VARGAS receives money pick-up contracts from OCEGUERA-TIRADO.

25. CS-1 has worked with DEA since 2019. Over the course of DEA-1's history of cooperating with the DEA, the information provided by CS-1 has led to multiple arrests and the seizure of multi-kilogram quantities of controlled substances, drug proceeds, and weapons. As detailed below, investigators have also independently corroborated the information provided by CS-1. As a result, investigators have deemed CS-1's information credible and reliable. CS-1 has no criminal history in the United States but has a prior conviction for money laundering in Mexico.

26. At the direction and control of case agents, CS-1 was able to insert himself/herself as a person capable of fulfilling money pickup contracts in the United States, converting the bulk currency to cryptocurrency, and delivering the cryptocurrency to its desired location. Beginning in September 2021, CS-1 began to receive money-laundering contracts from OCEGUERA-TIRADO and his sub-brokers, who were subsequently identified, including VELAZQUEZ-BRAVO, CUELLAR-FISHER and TORRES-ESPANA, in various cities across the United States in which CS-1, at the direction of MDO agents, would organize pick-ups of bulk cash which was then deposited into undercover Attorney General Exempt Operation (AGEO) accounts – undercover accounts which provide DEA the authority to conduct undercover financial transactions to infiltrate and dismantle DTMOs. After the bulk cash was deposited into undercover bank accounts, it was converted to Stable Coin and sent to cryptocurrency deposit addresses provided by OCEGUERA-TIRADO, VELAZQUEZ-BRAVO, CUELLAR-FISHER and/or TORRES-ESPANA. In addition to completing money contracts on behalf of OCEGUERA-TIRADO, VELAZQUEZ-BRAVO, CUELLAR-FISHER and/or TORRES-ESPANA, information obtained from OCEGUERA-TIRADO, VELAZQUEZ-BRAVO, CUELLAR-FISHER and/or TORRES-ESPANA money pick-ups have resulted in multiple seizures and/or arrests.²

² A money pick-up occurs when, in this case, a Mexico based money broker offers a contract to pick-up suspected drug proceeds in the United States, minus a commission, convert it to cryptocurrency, and transfer to the money broker.

C. Currency and Narcotics Seizures Associated with Money Laundering Contracts
Cocaine Seizure, Bulk Currency Seizure and Arrest on October 7, 2021

27. On or around September 15, 2021, OCEGUERA-TIRADO offered CS-1 a money laundering contract to pick up approximately \$200,000 in U.S. currency in Dallas, Texas, convert the U.S. currency to USDT (Stable Coin cryptocurrency), and transfer it to a USDT address provided by OCEGUERA-TIRADO. At the direction of agents, CS-1 accepted the contract and Milwaukee agents coordinated with DEA investigators in Dallas, Texas (DEA-TX) to complete the money pick-up. DEA agents in Texas, utilizing an undercover agent (UC), were telephonically contacted by an unknown male to arrange for the pick-up. This unknown male directed the UC to a home improvement store in Dallas, TX.

28. On September 17, 2021, DEA agents in Texas established surveillance in the area of the pre-determined location. Surveillance observed a Hispanic male, later identified as Vicente Jaimes-Garcia exit his vehicle and provide the UC with a bag determined to contain \$199,970 U.S. currency. On this same date, the U.S. currency received from Jaimes-Garcia was subsequently deposited into a DEA undercover account, converted to USDT, and sent to a deposit address, as directed by OCEGUERA-TIRADO through CS-1.

29. On October 6, 2021, OCEGUERA-TIRADO again offered a money laundering contract to CS-1 in Dallas, TX. The information was passed to DEA agents in Texas to assist in the pickup. On October 7, 2021, a UC made arrangements to pick up approximately \$200,000 and determined it was JAIMES-GARCIA who would again be delivering the U.S. currency. DEA agents in Texas subsequently stopped Jaimes-Garcia in route to the money pickup for a traffic violation. A consent search was conducted resulting in the seizure of \$199,810. Jaimes-Garcia agreed to a search of his residence, resulting in the seizure of seven kilograms of cocaine and an additional \$129,500 U.S

currency. Jaimes-Garcia was arrested and later released, pending indictment in the Northern District of Texas.

Fentanyl, Cocaine, and Bulk Currency Seizure on December 15, 2021

30. On or around December 3, 2021, VELAZQUEZ-BRAVO and CUELLAR-FISHER offered CS-1 a money laundering contract to pick up approximately \$150,000 in U.S. currency in Chicago, Illinois, convert the U.S. currency to USDT (Stable Coin), and transfer it to a USDT address provided by VELAZQUEZ-BRAVO and CUELLAR-FISHER. At the direction of case agents, CS-1 accepted the contract and Milwaukee agents coordinated with DEA investigators in Chicago, Illinois to complete the money pick-up. DEA agents in Illinois, utilizing an undercover agent (UC), was telephonically contacted by an unknown male to arrange for the pick-up. This unknown male and the UC agreed to meet at a home improvement store in Chicago, IL. On December 8, 2021, DEA agents established surveillance in the area of the pre-determined location. Surveillance observed a Hispanic male, later identified as Rodrigo Cortez exit his vehicle and provide the UC with a bag determined to contain \$145,000 U.S. currency.

31. On December 9, 2021, the U.S. currency received from Cortez was subsequently deposited into a DEA undercover account, converted to USDT, and sent to a deposit address, as directed by VELAZQUEZ-BRAVO and CUELLAR-FISHER through CS-1. On December 10, 2021, DEA agents established surveillance on Cortez at his residence in Chicago, Illinois. In the early evening, Cortez was approached, and the agents gained Cortez's consent to search his residence and vehicle. DEA agents recovered \$195,100 U.S. currency, approximately 10.6 kilograms of cocaine, approximately 1.3 kilograms of heroin, 200 grams of suspected Adderall pills in the residence and in an empty concealed compartment in the vehicle. Cortez was released and is subject to eventual prosecution in the Northern District of Illinois.

Cocaine and Bulk Currency Seizure on January 29, 2022

32. On or around December 3, 2021, VELAZQUEZ-BRAVO and CUELLAR-FISHER offered CS-1 a money laundering contract to pick up approximately \$100,000.00 in U.S. currency in Dallas, Texas, convert the U.S. currency to USDT (Stable Coin), and transfer it to a USDT address provided by VELAZQUEZ-BRAVO and CUELLAR-FISHER. At the direction of agents, CS-1 accepted the contract and MDO agents coordinated with DEA investigators in Dallas, Texas to complete the money pick-up. DEA agents in Texas, utilizing an undercover agent (UC), were telephonically contacted by an unknown male to arrange for the pick-up. This unknown male directed the UC to a location in Plano, Texas. On December 15, 2021, DEA established surveillance in the area of the pre-determined location. Surveillance observed a Hispanic male, later identified as Cesar Galicia-Cortes exit his vehicle and provide the UC with a bag determined to contain \$89,887 U.S. currency. On this same date, the U.S. currency received from Galicia-Cortes was subsequently deposited into a DEA undercover account, converted to USDT, and sent to a deposit address, as directed by VELAZQUEZ-BRAVO and CUELLAR-FISHER through CS-1.

33. On January 28, 2022, the DEA UC received a "cold call" from a target that wanted to deliver \$200,000 U.S. currency. DEA agents in Texas identified that the person who would be delivering the \$200,000 U.S. currency to the UC as Galicia-Cortes. On January 29, 2022, DEA agents established surveillance on Galicia-Cortes at his residence in Plano, Texas. A short time later, DEA agents, with the assistance of the Plano Police Department, conducted a traffic stop of Galicia-Cortes. During the traffic stop and an ensuing consent search of Galicia-Cortes' vehicle, DEA agents seized \$198,990 U.S. currency. During a post-*Miranda* interview of Galicia-Cortes, he provided written consent to search his residence in Plano, Texas, which resulted in the seizure of an additional \$202,873 U.S. currency in suspected narcotics proceeds, ten kilograms of cocaine, two semi-

automatic pistols, and multiple drug ledgers. Galicia-Cortes was processed at the scene and released pending further investigation but is subject to indictment in the Northern District of Texas.

D. Cryptocurrency Scheme and the Broker Accounts

34. Between on or around September 2021 and on or around December 2022, at the direction of OCEGUERA-TIRADO, VELAZQUEZ-BRAVO, CUELLAR-FISHER and/or TORRES-ESPANA, CS-1 has conducted more than 90 money laundering contracts resulting in cryptocurrency transfers. As part of these contracts, OCEGUERA-TIRADO, VELAZQUEZ-BRAVO, CUELLAR-FISHER and/or TORRES-ESPANA have provided CS-1 with several USDT³ deposit addresses to send USDT. The primary deposit address used by VELAZQUEZ-BRAVO and CUELLAR-FISHER and provided to CS-1 is 0x05e98039cf0a01a602b05bf2d1e4421d79f58096, a deposit address registered to the cryptocurrency exchange Huobi. During these transactions, case agents, by way of CS-1, have charged a 3% commission fee.

35. Between on or around December 8, 2021, and on or around June 3, 2022, DEA agents acting in an undercover capacity, conducted approximately 17 transactions in which a total of approximately 1,685,896.8 USDT (worth approximately \$1,686,317.51 in U.S. currency) was sent to the 0x05e98039cf0a01a602b05bf2d1e4421d79f58096 as directed by VELAZQUEZ-BRAVO and CUELLAR-FISHER. Subpoenaed records received from Huobi identified the account associated with the deposit address 0x05e98039cf0a01a602b05bf2d1e4421d79f58096 as a Huobi account belonging to Francisco Antonio GRANADOS-ARAQUE. The records list GRANADOS-ARAQUE's User ID as 268520016. The Huobi account was opened on or around October 16, 2021.

³ Based on my training and experience, I am aware that USDT is a stable coin cryptocurrency with a value meant to mirror the value of the U.S. dollar; USDT tokens are backed by offshore banks. Offshore banks offer fewer charges for operation and tax benefits, but they are not always fully secure like the FDIC-insured US banks.

Records further show between on or around October 19, 2021, and on or around March 4, 2022, approximately 10.13914888 BTC (worth approximately \$468,675.97 in U.S. currency) were deposited into the account, and approximately 3,199,000.422 USDT (worth approximately \$3,200,000 in U.S. currency) were deposited into the account for grand total of approximately \$3,668,675 U.S. currency deposited. During the same period approximately 3.9781 BTC (worth approximately \$183,885.24) were sent from GRANADOS-ARAQUE's account to other cryptocurrency addresses, and approximately 3,469,864.183 USDT (worth approximately \$3,470,000) were sent from the Huobi account to other cryptocurrency addresses.

36. The balance in the Huobi account on or around March 4, 2022, the date the records were provided, was effectively \$0.00. Analysis of the activity within the Huobi account shows that a large portion of the BTC and USDT deposited into the account was quickly converted to USDT and funds generally moved in and out of the account rapidly. Case agents believe the primary purpose of GRANADOS-ARAQUE's Huobi account, User ID 268520016, is to facilitate the DTMLO's money laundering activities by receiving drug proceeds into the account and moving it quickly to other cryptocurrency accounts for the purpose of money laundering.

37. Further analysis showed 3,385,774.369 USDT, or 97.5% of the withdrawn funds, went to the same wallet, TLNpEKGkUndcq4o4d5MEcfyQjyDFDgW4aD. On many occasions, the exact amount sent by DEA agents, acting in an undercover capacity, went from GRANADOS-ARAQUE's account to TLNpEKGkUndcq4o4d5MEcfyQjyDFDgW4aD. Therefore, case agents believe TLNpEKGkUndcq4o4d5MEcfyQjyDFDgW4aD is a deposit address controlled by GRANADOS-ARAQUE, VELAZQUEZ-BRAVO and/or CUELLAR-FISHER. At this time, case agents have not been able to connect TLNpEKGkUndcq4o4d5MEcfyQjyDFDgW4aD to an exchange service and believe it to consider an un-hosted wallet.

38. Based on my training and experience as well as my knowledge and information garnered from other money launderers in this case and similar cases, I know cryptocurrency transactions are often utilized to launder the proceeds derived from narcotic traffickers. More specifically, narcotics traffickers in source countries (e.g., Mexico and Colombia) provide narcotics to consumer countries (e.g., the United States). The bulk currency proceeds derived from the sale of these narcotics are then returned to the narcotics traffickers within the source countries utilizing various methods including the use of cryptocurrencies. In this case, the narcotic traffickers often contact brokers, or professional money launderers, who are responsible for collecting the bulk currency within the consumer countries and depositing the currency into the U.S. banking system. The brokers often then pay out the narcotics traffickers in fiat currency within the source countries, minus a commission, and sell the cryptocurrency to a separate “crypto” broker. The commission fee is generally between 3% and 5%. This crypto broker may then conduct a series of cryptocurrency transactions across multiple cryptocurrency exchanges utilizing an array of methods (e.g., cryptocurrency scrambler) in effort to obfuscate the true origin of the money. These crypto brokers often then sell the cryptocurrency in the “black market” in exchange for various fiat currencies.

THE TARGET ACCOUNTS

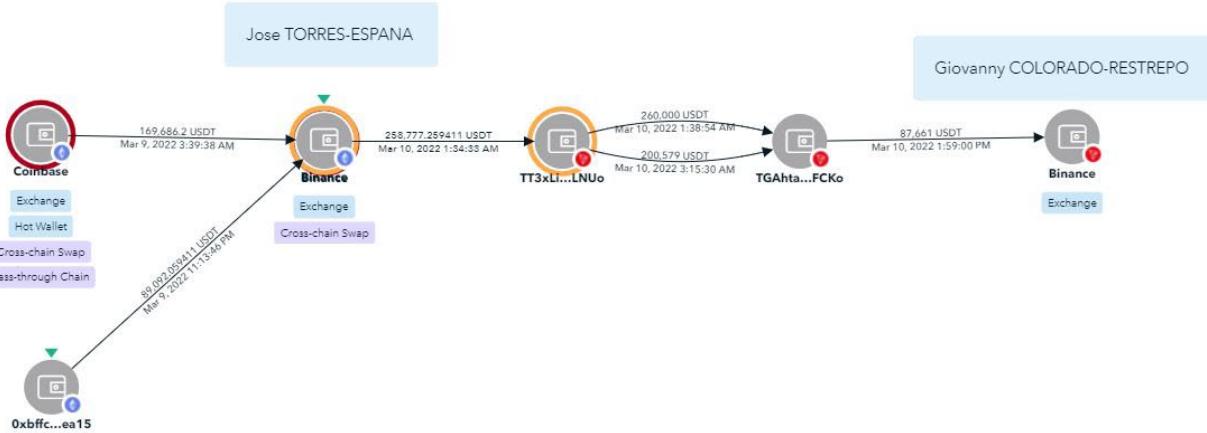
39. On or around March 4, 2022, TORRES-ESPANA offered CS-1 a money laundering contract to pick up approximately \$200,000 in U.S. currency in Chicago, Illinois, convert the U.S. currency to USDT (Stablecoin), and transfer it to a USDT address provided by TORRES-ESPANA. At the direction of agents, CS-1 accepted the contract and MDO agents coordinated with DEA investigators in Chicago, Illinois (DEA-IL) to complete the money pick-up. DEA agents in Illinois, utilizing an undercover agent (UC), were telephonically contacted by an unknown male to arrange for the pick-up. This unknown male directed the UC to a location in Chicago, IL. On March 8, 2022,

DEA agents established surveillance in the area of the pre-determined location. Surveillance observed a Hispanic male enter the front passenger seat of the UC vehicle. The Hispanic male provided the UC with a bag determined to contain \$175,000 U.S. currency. On this same date, the U.S. currency received from the Hispanic male was subsequently deposited into a DEA undercover account, converted to USDT, and sent 169,686.2 USDT to 0xB7eb7513356f393cc9bE056d57F186bB8E6c045b, as directed by TORRES-ESPANA through CS-1.

40. Subpoenaed records received from Binance identified the account associated with the deposit address 0xB7eb7513356f393cc9bE056d57F186bB8E6c045b as a Binance account belonging to Jose Humberto TORRES-ESPANA. The records list TORRES-ESPANA's User ID as 93580947. The account was opened on or around March 8, 2021. Records further show between on or around September 3, 2021, and on or around March 15, 2022, approximately 3,236,545.281 USDT (worth approximately \$3,236,000 in U.S. currency) were deposited into the account along with approximately \$82,473 in other cryptocurrencies. During the same period approximately 3,082,962.818 USDT (worth approximately \$3,082,000 in U.S. currency) and approximately \$254,255 in other cryptocurrencies were sent from the TORRES-ESPANA's account to other cryptocurrency addresses. The balance in TORRES-ESPANA's account on or around March 17, 2022, the date the records were provided, was effectively \$0.00.

41. On March 9, 2022, Binance records indicate TORRES-Espana also received 89,902.059411 USDT from wallet 0xbffce1ac879f8af65e59682c2396e8deb5fea15. On March 10, 2022, TORRES-Espana combined these two deposits and sent 258,777.259411 USDT to wallet TT3xLiAfDt8iXf3aoM3FprKdVC1To4LNUo. Public blockchain records revealed that on March 10, 2022, TT3xLiAfDt8iXf3aoM3FprKdVC1To4LNUo sent 260,000 USDT and an additional 200,579

USDT to wallet TGAhtavsbcsk1HNNa93v1ACWEe4W87FCKo. From there, the amounts were broken down even farther and continued to be transferred in smaller amounts to a multitude of wallets. On March 10, 2022, TGAhtavsbcsk1HNNa93v1ACWEe4W87FCKo sent 87,661 USDT to TTBpsGTJ31oUnBnP9KeGeZAPMfyv1MmAHf (**Target Account 1**).



42. On May 20, 2022, case agents subpoenaed Binance, requesting account information for TTBpsGTJ31oUnBnP9KeGeZAPMfyv1MmAHf (**Target Account 1**). On this same date, Binance responded that TTBpsGTJ31oUnBnP9KeGeZAPMfyv1MmAHf is a Binance deposit address associated with a Binance account belonging to Giovanny COLORADO-RESTREPO, Binance user ID 20963015, (**Target Account 1**). According to IP login information, COLORADO-RESTREPO commonly logs in from Bogota, Colombia and Medellin, Colombia. Based on their training and experience, and the investigation to date, case agents believe that a portion of the \$175,000 March 2022 money laundering contract was transferred to **Target Account 1**. Additionally, as discussed below, case agents believe that **Target Account 1** has historically been used to store the proceeds of money laundering contracts and to conceal and disguise the nature, location, source, and ownership of drug trafficking activities.

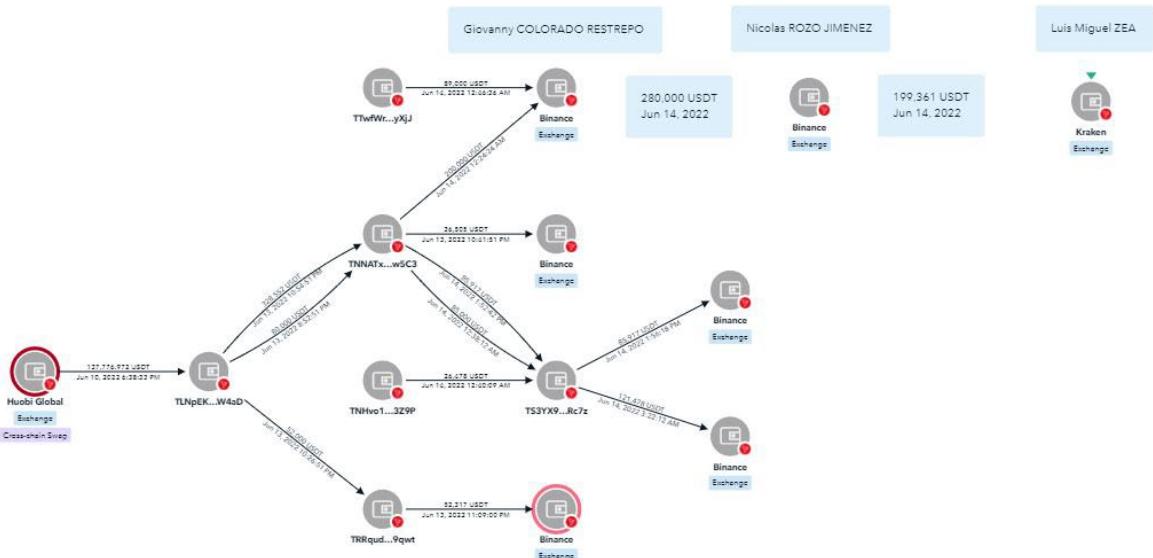
43. In January 2023 and April 2023, additional subpoenas were issued to Binance requesting information from **Target Account 1**. Analysis of **Target Account 1** revealed that between on or around January 6, 2021, and on or around March 29, 2023, **Target Account 1** received a total of 534 incoming deposits, mainly in USDT, totaling approximately \$31,434,375 in U.S. currency. Between January 6, 2021, and March 29, 2023, **Target Account 1** sent 320 outgoing withdrawals, totaling approximately \$22,422,813 in U.S. currency.

44. On or around June 2, 2022, VELAZQUEZ-BRAVO offered CS-1 a money laundering contract to pick up approximately \$100,000 in U.S. currency in Atlanta, Georgia, convert the U.S. currency to USDT, and transfer it to a USDT address provided by VELAZQUEZ-BRAVO. At the direction of agents, CS-1 accepted the contract and MDO agents coordinated with DEA investigators in Atlanta, Georgia (DEA-GA) to complete the money pick-up. DEA agents in Georgia, utilizing an undercover agent (UC), were telephonically contacted by an unknown male, later identified as Juan Manuel CONTRERAS-PAVON, to arrange for the pick-up. CONTRERAS-PAVON directed the UC to a location in Stockbridge, GA. On June 3, 2022, DEA agents established surveillance in the area of the pre-determined location. Surveillance observed CONTRERAS-PAVON enter the front passenger seat of the UC vehicle. CONTRERAS-PAVON provided the UC with a bag determined to contain \$100,000 U.S. currency. On June 6, 2022, the U.S. currency received from CONTRERAS-PAVON was subsequently deposited into a DEA undercover account, converted to USDT, and sent 97,066.6 USDT to 0x05E98039cF0a01A602b05BF2D1E4421d79f58096, the previously mentioned Huobi account registered to GRANADOS-ARAQUE, as directed by VELAZQUEZ-BRAVO through CS-1.

45. According to Huobi records, on June 9, 2022, GRANADOS-ARAQUE also received 29,915 USDT from wallet 0x0f73f8347b2f851cf03daafb0f1010f219bcd55 and on June 10,

2022, the account received 2,000 USDT from 0x0f73f8347b2f851cf03daafb0f1010f219bcd55. On June 10, 2022, GRANADOS-ARAQUE's account combined the three deposits and sent 137,776.972 USDT to wallet TLNpEKGkUndcq4o4d5MEcfyQjyDFDgW4aD, an unhosted wallet believed to also be used by GRANADOS-ARAQUE. Public blockchain records reveal that on June 13, 2022, TLNpEKGkUndcq4o4d5MEcfyQjyDFDgW4aD sent 80,000 USDT and a second transfer of 328,552 USDT to TNNATxMZvvmdCC3Y7PrsxVCMLYBuPow5C3, an unhosted wallet. On June 14, 2022, TNNATxMZvvmdCC3Y7PrsxVCMLYBuPow5C3 sent 200,000 USDT to TTBpsGTJ31oUnBnP9KeGeZAPMfyv1MmAHf, **Target Account 1**, registered to Giovanny COLORADO-RESTREPO. Binance records reveal that on June 14, 2022, **Target Account 1** combined the previously mentioned 200,000 USDT and a second deposit of 80,000 USDT and sent 280,000 USDT to TEAUG83rLm8JsttvBYvu4SKPMuQaXQYmE4 (**Target Account 2**), registered to Nicolas ROZO-JIMENEZ. From there, ROZO-JIMENEZ sent 199,341 USDT to TA4KrrnpytSobDr6hxzE8YurxqcP5AiPCj, a Kraken deposit address, registered to Luis Miguel ZEA.

46. In December 2022, case agents issued an administrative subpoena to Kraken, who responded that the Kraken deposit address TA4KrrnpytSobDr6hxzE8YurxqcP5AiPCj is registered to ZU Capital Inc, with an email address of zucapitalinc@gmail.com and registered owner of Luis Miguel ZEA and address of 225 Deer Creek Blvd, Apt. 901, Deerfield Beach, FL. On March 7, 2023, Kraken records reveal that the account was closed by Kraken due to "potential money laundering associated with a known Colombian money mule typology."



47. DEA Atlanta agents continued the investigation and identified Juan CONTRERAS and his son, Juan CONTRERAS-PAVON, as large-scale money launderers, who, since January 2022, have laundered an estimated \$1 million U.S. currency back to Mexico. Based on the intelligence and evidence gained to date in that investigation, as well as the probable cause developed by the bulk currency pick-up on June 3, 2022, Atlanta agents obtained authorization to execute two federal search warrants at residences controlled by CONTRERAS. On June 10, 2022, while conducting surveillance on CONTRERAS, agents observed CONTRERAS-PAVON meet with CONTRERAS in the same manner in which they met prior to CONTRERAS-PAVON delivering \$100,000 to the UC during the June 3 bulk currency pick-up.

48. Based on case agents' knowledge of the inner workings of this DTMLO, the Georgia State Patrol (GSP) conducted a traffic stop on CONTRERAS-PAVON. During a probable cause search of CONTRERAS-PAVON's vehicle, GSP troopers seized THC vape pens, a 9mm pistol, a 2015 Chevrolet Camaro, and \$300,055 U.S. currency. CONTRERAS-PAVON was arrested for felony possession of the THC vape pens, as well as felony possession of a firearm during the commission of a crime. Subsequently, Atlanta FD agents executed the federal search warrants at the two residences

in Stockbridge, GA, and coordinated a stop/approach of CONTRERAS. During the approach of CONTRERAS, and consensual search of CONTRERAS' vehicle, agents seized a 9mm handgun. Inside the money stash house, Atlanta FD agents seized \$993,493 U.S. currency and two money counters. Inside the residence of CONTRERAS and CONTRERAS-PAVON, Atlanta FD agents seized \$13,256 U.S. currency, approximately 1/3 kilogram of suspected cocaine, four additional THC vape pens, approximately 74 grams of marijuana, two handguns, one rifle, and one shotgun. Charges on CONTRERAS and CONTRERAS-PAVON are pending.

49. In April 2023, case agents sent an administrative subpoena to Binance, requesting account information for **Target Account 2**. Binance responded that deposit address TEAUG83rLm8JsttvBYvu4SKPMuQaXQYmE4 is associated with Binance User ID 197016535, registered to Nicolas ROZO-JIMENEZ. According to IP login information, ROZO-JIMENEZ commonly logs in from Bogota, Colombia. Between January 24, 2022, and April 24, 2023, **Target Account 2** received a total of 571 incoming deposits, mainly in USDT, totaling approximately \$40,341,278 in U.S. currency. Of these incoming transactions, 139 of the deposits were sent from **Target Account 1**, totaling approximately \$12,862,248. Between January 11, 2022, and April 24, 2023, **Target Account 2** sent 332 outgoing withdrawals, totaling approximately \$40,359,679 in U.S. currency.

50. Further review of **Target Account 2** revealed three incoming deposits, totaling approximately \$107,484, from deposit address TT3JryrlsVbMRc6f15n7Py3nYq4yWoCrMn. Law enforcement database checks revealed the deposit address TT3JryrlsVbMRc6f15n7Py3nYq4yWoCrMn was provided to a DEA New York confidential source to send \$112,000 from a money pickup in December 2022 for the purpose of money laundering. Additionally, deposit address TUu2f3T5WRMBW8yAieTiHtvFizp6GtZASj sent two deposits,

totaling approximately \$178,438 in U.S. currency to **Target Account 2**. TUu2f3T5WRMBW8yAieTiHtvFizp6GtZASj has sent transactions previously to TT3Jryr1sVbMRc6f15n7Py3nYq4yWoCrMn. TT3Jryr1sVbMRc6f15n7Py3nYq4yWoCrMn has also sent 9 deposits to **Target Account 1** totaling approximately \$835,876 in U.S. currency.

51. As previously mentioned, between January 24, 2022, and April 24, 2023, **Target Account 2** received 139 deposits from **Target Account 1**, totaling approximately \$12,862,248 U.S. currency. The interactions between **Target Account 1** and **Target Account 2** seemed to decline beginning in March 2023. Beginning in January 2023, but significantly increasing in activity beginning March 2023, **Target Account 3** sent 35 deposits to **Target Account 2** totaling approximately \$2,016,015 U.S. currency.

52. In April 2023, case agents sent an administrative subpoena to Binance, requesting account information for **Target Account 3**. Binance responded that deposit address TFsG7i3i66cSUFfjPsUkRBJPJFSg3Vm455 is associated with Binance User ID 27815331, registered to Juan Esteban ARDILA-LONDONO. According to IP login information, ROZO-JIMENEZ commonly logs in from Medellin, Colombia and Bogota, Colombia. Between February 23, 2022, and April 24, 2023 (however the bulk of activity was between February 9, 2023, and April 24, 2023), **Target Account 3** received a total of 52 incoming deposits, all in USDT, totaling approximately \$2,501,124 U.S. currency. Of these incoming transactions, one of the deposits was sent from **Target Account 1**, totaling approximately \$59,994 U.S. currency and five of the deposits was sent from **Target Account 2**, totaling approximately \$26,239 U.S. currency. Between February 6, 2022, and April 24, 2023, **Target Account 2** sent 69 outgoing withdrawals, totaling approximately \$2,413,472 U.S. currency. Of these outgoing transactions, 35 withdrawals, totaling approximately

\$2,016,015, was sent to **Target Account 2** and one withdrawal, totaling approximately \$27,499 U.S. currency was sent to **Target Account 1**.

53. Analysis of the **Target Accounts** revealed **Target Account 1** had a significant drop-off of activity in March 2023. In April 2023, case agents contacted Binance, who advised agents that Binance had locked and removed **Target Account 1** on March 30, 2023. Binance's anti-money laundering team had independently reviewed **Target Account 1** and locked the account due to three reasons:

- A. Multiple counter party transactions with other law enforcement flagged accounts;
- B. Rapid movement of funds flowing through the account, with no trading activity; and
- C. A conclusion that the "Know Your Customer" photo sent in by COLORADO-RESTREPO was fraudulent based upon a review of the metadata.

54. Based upon the significant drop-off in activity from **Target Account 1**, due to the account being locked by Binance, and then the rapid acceleration of use in **Target Account 3**, case agents believe **Target Account 3** is a replacement account for **Target Account 1** and is being used in furtherance of the money laundering conspiracy.

55. A significant sample of the **Target Accounts** have been further reviewed, and display characteristics of money laundering activity including but not limited to the following:

- A. Rapid movement of cryptocurrencies into and out of the accounts over short periods of time;
- B. Large dollar equivalent amounts of cryptocurrency transactions in and out of the accounts that often, but not always, result in a near net zero or relatively small dollar ending balance;
- C. A flow of cryptocurrency funds to user accounts owned by individuals in narcotic source countries (e.g., Mexico, Colombia), consistent with transactions DEA has observed in undercover operations as previously described; and
- D. Accounts with relatively little or no deposits or withdrawals of fiat currency into or from the accounts.

56. Based on training and experience, and the investigation to date, case agents believe the aforementioned characteristics are indicative of the **Target Accounts** being used to facilitate the movement of illegal proceeds derived from the sale of narcotics and obfuscate the true origin of the funds.

IV. CONCLUSION

57. Based upon all of the foregoing, there is probable cause to believe that the **Target Accounts** held by Binance Holdings Limited (“Binance”) contain property traceable to the distribution and sale of narcotics in violation of Title 21, United States Code, Section 841, et. seq., and/or are property involved in money laundering and unlicensed money transmitting in violation of Title 18, United States Code, Section 1956 and Section 1960, respectively.

58. Title 18, United States Code, Section 1956 makes it unlawful, in part, to conduct a financial transaction, knowing that the property involved in the financial transaction represents the proceeds of some form of specified unlawful activity, knowing that the transaction is designed in whole or part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

59. Likewise, Title 18, United States Code, Section 1960 makes it unlawful to engage in an unlicensed money transmitting business. An unlicensed money transmitting business is defined as one which affects interstate or foreign commerce in any manner or degree, is operated without an appropriate license in a state, whether or not the transmitter knew that the operation was required to be licensed, is not in compliance with the money transmitting business registration requirements under 31 U.S.C. § 5330, which requires that money transmitting businesses be registered with the Secretary of the Treasury, or otherwise involves the transportation or transmission of funds that are

known by the transmitter to have been derived from a criminal offense, or are intended to be used to promote or support unlawful activity.

60. Accordingly, I submit that there is probable cause to support the issuance of a warrant to civilly and criminally seize up to approximately 456,995.14843 USDT held in the Binance account belonging to Nicolas ROZO-JIMENEZ, Binance user ID 197016535 (“**Target Account 2**”), and up to approximately 60,000 USDT held in the Binance account belonging to Juan Esteban ARDILA-LONDONO, Binance User ID 27815331 (“**Target Account 3**”) pursuant to Title 21, United States Code, Section 881(a)(6) (civil forfeiture of drug proceeds); Title 18, United States Code, Section 981(a)(1)(A) (civil forfeiture of property involved in money laundering and unlicensed money transmitting); Title 21, United States Code, Section 853 (criminal forfeiture of drug proceeds); and Title 18, United States Code, Section 982(a)(1) (criminal forfeiture of property involved in money laundering and unlicensed money transmitting). Furthermore, since the underlying conspiracy is ongoing, there is probable cause to believe that further illicit proceeds subject to seizure will transferred to **Target Account 2** and **Target Account 3** in the days subsequent to the service of an approved seizure warrant on Binance. For this reason, I request Binance be directed to seize all incoming funding deposits or transfers to **Target Account 2** and **Target Account 3** specified in Attachment A for a period of three (3) days after the seizure warrant is served.

61. The Court has authority to issue seizure warrants for property located outside the Eastern District of Wisconsin, pursuant to Title 18, United States Code, Section 981(b)(3). Section 981(b)(3) provides that a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action may be filed under Title 28, United States Code, Section 1355(b), “and may be executed in any district in which the property is found. . . .” Title 18 U.S.C. § 981(b)(3). In turn, Title 28, United

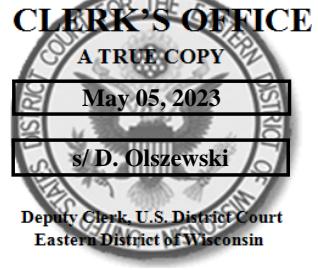
States Code, section 1355(b) provides that a forfeiture action may be brought in any district where any of the underlying acts or omissions occurred upon which the forfeiture based.

ATTACHMENT A

All items of value, including fiat currency and all forms of cryptocurrency, held in the accounts associated with the User IDs located at Binance Holdings Limited identified below with permission to serve the warrant electronically followed by original service.

Binance is instructed to allow incoming funds but not allow funds to be withdrawn, transferred, wired, routed or otherwise disbursed by or to any persons (other than the federal agents authorized to seize the funds) for a period of three (3) days from the issuance of the warrant.

- A. Approximately 456,995.14843 USDT held in the Binance account belonging to Nicolas ROZO-JIMENEZ, Binance user ID 197016535 (“Target Account 2”); and**
- B) Approximately 60,000 USDT held in the Binance account belonging to Juan Esteban ARDILA-LONDONO, Binance User ID 27815331 (“Target Account 3”).**



UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF WISCONSIN

In the Matter of the Seizure of

(Address or brief description of property or premises to be seized)

APPROXIMATELY 456,995.14843 USDT, AND ANY OTHER FIAT CURRENCY AND ALL FORMS OF CRYPTOCURRENCY, ON DEPOSIT IN BINANCE ACCOUNT USER ID #197016535, HELD IN THE NAME OF NICOLAS ROZO-JIMENEZ

Case Number: 23 MJ 75

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

TO: **KELLEN J. WILLIAMS, a Special Agent with the Drug Enforcement Administration, and any Authorized Officer of the United States.**

An application by a federal law enforcement officer or an attorney for the government requests that certain property be seized as being subject to forfeiture to the United States of America. The property is described as follows:

Approximately 456,995.14843 USDT, and any other fiat currency and all forms of cryptocurrency, on deposit in Binance account user ID #197016535, held in the name of Nicolas Rozo-Jimenez

I find that the affidavit and any recorded testimony establish probable cause to seize the property.

YOU ARE HEREBY COMMANDED to search on or before 5/19, 2023
(not to exceed 14 days)

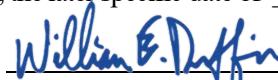
in the daytime – 6:00 a.m. to 10:00 p.m. at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge William E. Duffin.

I find that immediate notification may have an adverse result listed in 18 U.S.C. §2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person, who, or whose property, will be searched or seized (check the appropriate box) for _____ days. (not to exceed 30)
 until, the facts justifying, the later specific date of _____

Date and time issued 5/5, 2023; 1:49 p.m.



Judge's signature

City and state: Milwaukee, Wisconsin

THE HONORABLE WILLIAM E. DUFFIN
United States Magistrate Judge
Name & Title of Judicial Officer

Return

| | | |
|------------------------------------|---------------------------------|--|
| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
| Inventory made in the presence of: | | |
| Inventory of the property taken: | | |

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title